

ReturnCase No.:
23-m-329 (SCD)

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

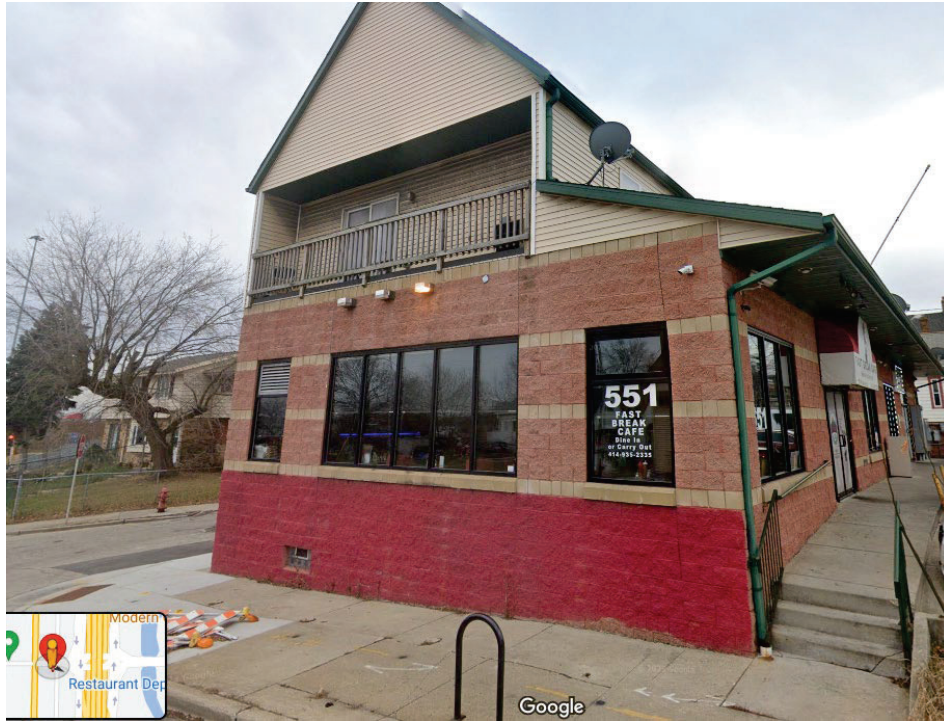
ATTACHMENT A

Property to Be Searched

551 West Becher Street, #A and #B, Milwaukee, Wisconsin, to include all associated common spaces, basement, garage, outbuildings, and a **Dodge Durango bearing Indiana registration plates of FL386ACC**, at this address. Apartments #A and #B are located on the second floor of a dwelling and above two businesses. The ground entry door is on the east side of the building near the south corner. There is a staircase upon opening the ground entry door that runs north to south. Once at the top of the stairs, there is a door to the left and a door straight ahead. The door straight ahead is Apartment #A, while the door to the left is Apartment #B. Apartment #A occupies the northern part of the second floor while Apartment #B occupies the southern part of the second floor.



(Ground access door)



(North side of Building)



(2013 Photograph – Apartment #A straight ahead and Apartment# B on left)

ATTACHMENT B

Property to be seized

1. Evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (Distribution of and possession with intent to distribute controlled substances), and 846 (Conspiracy to distribute and possess with intent to distribute controlled substances), those violations involving Ricky T. MERRITT, including:

- a. Controlled substances, controlled substance analogues, or listed chemicals;
- b. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
- c. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
- d. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
- e. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
- f. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;
- g. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and

other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

- h. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
 - i. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
 - j. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;
 - k. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;
 - l. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;
 - m. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and
2. Computers, cellular telephones, or storage media used as a means to commit the violations described above;
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in

which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

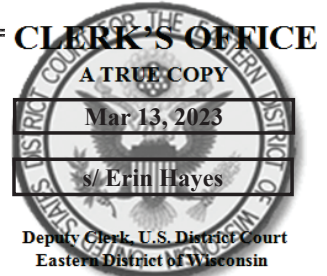
As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MERRITT to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of MERRITT’s face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)551 West Becher Street, #A and #B, Milwaukee, Wisconsin, to include all
associated common spaces, basement, garage, outbuildings, and a
Dodge Durango bearing Indiana registration plates of FL386ACC, at this
address, as further described in Attachment A.

Case No.

23-m-329 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841(a)(1) & 846	Distribution of controlled substances & Conspiracy to possess with intent to distribute and to distribute controlled substances

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DEA TFO James Enters

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ telephone (specify reliable electronic means).

Date: 3-13-23

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A WARRANT TO SEARCH AND SEIZE**

I, James Enters, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as **551 West Becher Street, #A and #B, Milwaukee, Wisconsin**, hereinafter "**SUBJECT PREMISES**," further described in Attached A, for the things described in Attachment B.

2. I am a federally deputized Task Force Officer (TFO) with the Drug Enforcement Administration (DEA). I have been a DEA TFO with North Central High Intensity Drug Trafficking Areas (HIDTA) since January of 2022 and have approximately nine years of law enforcement experience with the Greenfield Police Department. Over that collective period, I have participated in both long-term and short-term narcotics investigations. I have had extensive training in the investigation of drug trafficking from the Greenfield Police Department, Drug Enforcement Administration, and the Wisconsin Department of Justice, Division of Criminal Investigation (DCI). Through these investigations, my training and experience, and conversations with other law enforcement personnel, I have become familiar with the methods used by drug traffickers to manufacture, smuggle, safeguard, and distribute narcotics, and to collect and launder trafficking-derived proceeds. I am further aware of the methods employed by major narcotics organizations to thwart any investigation of their illegal activities.

3. Based on my training, experience, and conversations with other law enforcement officers (LEOs), I am familiar with the ways in which drug traffickers conduct their unlawful drug trafficking activity, including, but not limited to, their methods used to distribute, transport, store, and import controlled substances, their use of code words and numbers to conduct their transactions, their methods for concealing and safeguarding narcotics and narcotics proceeds, their methods used to launder narcotics proceeds, and their use of violence and threats of violence to protect their organization. For example, I am familiar with their use of telephones, counter-surveillance, false and/or fictitious identities, the use of coded language during conversations when referring to narcotics in an attempt to disguise the true meaning of the conversation, and the use of vehicles to transport controlled substances and conduct mobile drug transactions.

4. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

5. To this end, based upon my training and experience, I know that individuals involved in drug trafficking frequently use cellular telephones to maintain

contact and arrange transactions with their sources and customers of and co-conspirators in the distribution of controlled substances. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in "text" format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs. I also believe that it is common for crime suspects who possess illegal controlled substances and firearms to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and firearms that they control, possess, buy, and sell.

6. The facts in this affidavit come from my personal observations, my training and experience, my review of oral and written reports of other law enforcement officers participating in this and related investigations, records, documents, and other evidence obtained during this investigation. The investigation to date has involved traditional law enforcement methods, including, but not limited to confidential informants, interviews, and physical and electronic surveillance.

7. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

PROBABLE CAUSE

9. The United States, including the DEA and the Milwaukee Metropolitan Drug Enforcement Group, are conducting a criminal investigation of Ricky T. MERRITT (DOB: 06/15/1985) regarding possible violations of Title 21, United States Code, Sections 841(a)(1) (distribution of and possession with intent to distribute controlled substances) and 846.

10. In early March of 2023, an individual later identified as a confidential informant (CI) was arrested for distribution of fentanyl, stemming from two controlled purchases of fentanyl from the CI. These controlled purchases occurred on or about January 12, 2023, and on or about February 2, 2023. During the first controlled purchase, approximately 25.64 grams of fentanyl was obtained from the CI. During the second controlled purchase, approximately 49.87 grams of fentanyl was obtained from the CI.

11. Based upon my training and experience, I know that a “controlled buy” is a law enforcement operation in which a confidential source purchases drugs from a target. The operation is conducted using surveillance, usually audio and video recording equipment, and pre-recorded purchase money. When a confidential source is used, s/he is searched for contraband, weapons, and money before the operation. The confidential source is also equipped with a recording and monitoring device. When the transaction is completed, the confidential source meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The confidential source is again searched for contraband, weapons, and money. The recording equipment is reviewed to determine consistency with confidential source

statements and law enforcement surveillance. A sample of the suspected drugs is then field tested by case agents for the presence of controlled substance and then placed in inventory pursuant to normal inventory procedures.

12. After the CI's arrest, a *Mirandized* interview of the CI was conducted. The CI stated that the CI does not live in Milwaukee but has been coming to Milwaukee since 2016. The CI stated the CI came to Milwaukee approximately once per week and stayed approximately four days at a time. The CI stated that the CI came to Milwaukee to traffic controlled substances, including heroin and fentanyl. The CI stated that the CI was supplied controlled substances by an individual known to the CI as "Ricky." The CI was shown a photograph of Ricky T. MERRITT (DOB: 06/15/1985) and the CI positively identified MERRITT as the individual who supplied the CI with heroin and/or fentanyl to sell in the City of Milwaukee. The CI has known MERRITT for approximately eight months, and MERRITT has been the CI's sole source of supply for controlled substances.

13. The CI stated that MERRITT lives in an apartment above Fast Break Café located at **551 West Becher Street**, the **SUBJECT PREMISES**. The CI stated that there are two apartments above the café and the only access door for the apartments is on the southeast corner of the building. The CI stated that the CI has a key for the main access door on the southeast corner, but the CI does not have a key to the apartments at the top of the stairs. The CI stated that upon entering the ground level entry door of the **SUBJECT PREMISES**, there is a staircase to the right. Upon going up the staircase, there is a landing. Once on the landing there is a door on the left and there is a door straight ahead. The door on the left is believed to be the southernmost apartment (**Apartment B**) while

the door on the right is believed to be the northernmost apartment (**Apartment A**). The southernmost apartment is located on the floor above a coin laundry mat while the northernmost apartment is located on the floor above the café. The CI stated that MERRITT resides and sleeps in the northernmost apartment, however, MERRITT keeps personal belongings and his four dogs in the southernmost apartment. The CI stated that MERRITT has keys for both apartments. The CI has further been in both apartments with MERRITT. The CI stated that MERRITT's aunt will occasionally stay in the southern apartment, but she is not there often.

14. The CI stated that MERRITT owns four Pit bull dogs that the CI believes to be vicious by the way they act. The CI stated that MERRITT will commonly keep the dogs in the staircase area during normal sleeping hour for protection and to alert him (MERRITT) if someone is at the ground access door. Based on case agents' knowledge of controlled substance trafficking cases, case agents know that traffickers often use dogs for protection in their personal residence or where they keep illegal contraband.

15. The CI stated that the CI has purchased cocaine, crack cocaine, heroin, and fentanyl from MERRITT. The CI stated that the controlled substance transactions occurred in the northernmost apartment, believed to be **Apartment A**. The CI stated that the CI's customers customarily ordered two hundred to three hundred grams of a specific controlled substance from the CI. The CI then contacted MERRITT to place the order for the specific controlled substance the CI's customers want. After MERRITT procured the controlled substance, the CI met with MERRITT in **Apartment A**, at which time the CI obtained the controlled substances from MERRITT. According to the CI, MERRITT

usually “fronted” the controlled substances to the CI, meaning MERRITT distributed the controlled substances to the CI and did not collect payment until a later time. Subsequently, the CI left to sell the controlled substances to the CI’s customers. After selling the controlled substance, the CI brought MERRITT U.S. currency to pay for the controlled substances, and the CI received a profit from the sale. According to the CI, the CI always brought the U.S. currency made from the narcotics sales back to **Apartment A**. The CI stated that the CI has been coming to Milwaukee approximately once a week to obtain controlled substances from MERRITT since they met approximately 8 months ago.

16. The CI stated that in the end of February 2023, the CI observed one to two kilograms of cocaine in MERRITT’s northernmost apartment, believed to be **Apartment A**, and MERRITT was breaking the cocaine into quantities consistent for sale. As described below, court-authorized vehicle GPS location reflects that the CI’s vehicle was in the vicinity of the **SUBJECT PREMISES** on February 28, 2023. According to the CI, while inside the **SUBJECT PREMISES**, the CI has observed MERRITT in possession of a Glock handgun on numerous occasions. The CI stated that MERRITT will sometimes carry the firearm with him in public or sometimes keep it in the **SUBJECT PREMISES**.

17. Before being arrested, the CI stated the CI was on the way to Milwaukee to talk to MERRITT about a future order of controlled substances for their clients and because MERRITT wanted to purchase a kilogram press for his controlled substances. The CI previously told MERRITT that the CI would be able to purchase a press for MERRITT.

18. The CI has been cooperating with law enforcement since March 2023. The CI has made statements against the CI's penal interest. The CI has three felony controlled substance-related convictions, including two convictions for manufacturing or delivering a controlled substance and one conviction for the possession of a controlled substance. The CI also has a conviction for possessing a weapon as a convicted felon and a misdemeanor assault conviction. The CI is cooperating for consideration on the criminal charges that have yet to be issued by the United States for the above-described purchases of controlled substances from the CI. Thus far, the information provided by the CI has been corroborated by information known to case agents. The CI's information has also been corroborated by law enforcement through independent investigation. More specifically, the CI's information has been corroborated by digital surveillance video, physical surveillance, court-authorized vehicle GPS data from the CI's vehicle, consensually recorded conversations, controlled buys, and digital evidence contained on the CI's cell phone, and more specifically, the CI's text messages. Within the context of the information detailed and relied upon for purposes of this Affidavit, case agents believe the CI is credible and the CI's information reliable.

Electronic and Physical Surveillance

19. On January 26, 2023, the Honorable Milwaukee County Circuit Court Judge Jack L. Davila signed an Order authorizing the use of a Global Positioning System (GPS) tracking device on the CI's vehicle. The vehicle GPS data from the CI's vehicle reflected that the CI's vehicle was in the City of Milwaukee during the following dates: January 26 -29, February 1-5, February 10-18, February 22-23, and February 28.

20. Within the time periods the CI's vehicle was in Milwaukee, the location data showed the vehicle to be within approximately two blocks of the **SUBJECT PREMISES** at some point during the CI's stay. Case agents located and observed the CI's vehicle parked near South 7th Street and West Becher Street. Case agents believed that the CI would park a short distance from the house to distance the CI's vehicle from the **SUBJECT PREMISES**. Case agents know narcotics traffickers will do this so law enforcement cannot associate their vehicle with the residence they frequent.

21. While case agents were investigating the CI for trafficking controlled substances, and before the CI was arrested, case agents conducted physical surveillance on the CI. On February 1, 2023, case agents observed the CI operate the CI's vehicle and park in the parking lot located at **551 West Becher Street**, the **SUBJECT PREMISES**. As previously stated, located at **551 West Becher Street** is a diner named Fast Break Café. The café is connected to a coin laundromat that has an address of 555 West Becher Street. There are apartments above the businesses, and MERRITT has access to both apartments. At approximately 2:11 p.m., the CI entered the café. The CI left in the CI's vehicle at approximately 2:38 p.m. The CI was then followed to the 2100-block of South Robinson Avenue where the CI parked at approximately 2:41 p.m. At approximately 2:55 p.m., the CI left in the CI's vehicle and was followed by a silver Jeep Gladiator bearing Wisconsin registration plates of RX-3680. Shortly thereafter, both vehicles parked at approximately 222 East Clifford Street. Case agents observed the CI exit the CI's vehicle and enter the silver Jeep Gladiator. Based on their training, experience, and familiarity with this investigation, case agents believe this to be suspicious behavior because case agents know

that individuals engaged in criminal activities will park their vehicles away from their residence to prevent law enforcement from identifying where they live.

22. During this time, case agents were receiving E911 location data for the CI's cell phone. This data was being received pursuant to a court Order that was signed on January 20, 2023, by the Honorable Milwaukee County Circuit Court Judge Glenn Yamahiro. During normal sleeping hours between February 1 to February 2, the location data reflected that the CI's cell phone was in the area of the **SUBJECT PREMISES**. At approximately 7:00 a.m. on February 2, 2023, case agents observed that the CI's vehicle was still parked at 222 East Clifford Street. Case agents then went to the **SUBJECT PREMISES**. Case agents observed the silver Jeep Gladiator parked in the alley behind the **SUBJECT PREMISES**, which alley is on the south side of the building. The silver Jeep Gladiator was parked up against the building. Case agents observed a door on the southeast corner of the building. There were two mailboxes to the right of the door that were labeled with "A" and "B" on the mail boxes.

23. On February 2, 2023, at approximately 10:00 a.m., case agents observed the CI, MERRITT, and a third unidentified male exit the door on the southeast corner of the building. MERRITT entered the driver seat of the Jeep Gladiator and the CI entered the rear passenger seat. The third unidentified male walked away from the location.

24. On February 8, 2023, case agents conducted physical surveillance on the **SUBJECT PREMISES**. Case agents observed a gray 2021 Toyota Highlander bearing Florida registration plates of LDLQ04. A registration check found the vehicle is owned by EAN Holdings LLC (Enterprise). Case agents contacted Enterprise and found that

MERRITT rented the vehicle on January 16, 2023 and was due to return the vehicle on February 17, 2023.

25. Through case agents' training and experience in conducting controlled substance trafficking investigations, case agents know narcotics traffickers use rental vehicles, believing that it makes it more difficult for law enforcement to identify who is driving and in control of the vehicle. Case agents further know that traffickers also frequently switch rental vehicles to make it even more difficult for law enforcement to identify which car the individual is driving.

26. On February 12, 2023, case agents conducted digital surveillance of the **SUBJECT PREMISES**. At approximately 4:03 p.m., case agents observed the gray Toyota Highlander arrive and park on the east side of South 5th Place. Case agents observed MERRITT and the CI exit the vehicle and walk through the alley and to the west side of the building.

27. On February 14, 2023, case agents conducted digital surveillance of the **SUBJECT PREMISES**. At approximately 8:26 a.m., case agents observed the CI exit the southeast door and enter the gray Toyota Highlander. The CI operated the vehicle away from the location. At approximately 9:00 a.m., the Highlander returned and the CI used a key to enter the southeast door to access the **SUBJECT PREMISES**. At approximately 11:55 a.m., case agents observed MERRITT and an unidentified female exit the **SUBJECT PREMISES** and walk to the gray Highlander. They attempted to open the doors of the vehicle but the doors appeared locked. They both then walked back towards the **SUBJECT PREMISES**, and MERRITT used a key to open the southeast door. Shortly

thereafter, MERRITT and the unidentified female exited the southeast door and entered the gray Highlander and drove away.

28. On February 15, 2023, case agents conducted digital surveillance of the **SUBJECT PREMISES**. At 2:27 a.m., case agents observed the gray Highlander park behind the **SUBJECT PREMISES**. MERRITT and an unidentified female exited the vehicle, and MERRITT used keys to open the southeast access door of the building. At 10:45 a.m., case agents observed MERRITT and the same unidentified black female exit the southeast access door and enter the Toyota Highlander. MERRITT then drove the vehicle away from the location.

29. On February 17, 2023, case agents conducted digital surveillance of the **SUBJECT PREMISES**. At 10:53 a.m., MERRITT exited the southeast access door and entered the gray Highlander. MERRITT exited the vehicle shortly after and was in possession of a large black and white checkered bag or package. MERRITT held this bag tightly against his body under his right arm. MERRITT walked west in the alley out of the view of digital surveillance. At 10:55 a.m., case agents observed MERRITT walking east in the alley behind the building, and MERRITT was carrying a red bag that appeared to be heavy based on the appearance of the bag. MERRITT was no longer carrying the black and white checkered bag. While MERRITT was walking, MERRITT was very alert and attentive as he was looking around and over his shoulder before he entered the gray Highlander.

30. Based on case agents' experience in investigating controlled substance trafficking offenses and conducting surveillance of trafficking activities, case agents

know that transactions are commonly done in secluded areas like an alley to hide the illegal transaction. MERRITT was first seen with the black and white checkered bag and then returned with a different red bag. Based on these observations, and their training and experience, case agents believe that MERRITT conducted an illegal controlled substance transaction. Case agents further know that individuals are often very alert while in possession of illegal contraband while in public to detect the presence of law enforcement or individuals who wish to deprive them of their contraband. Based on the appearance of the bag and MERRITT's mannerisms, case agents believed that illegal contraband was in the bag and that MERRITT used his vehicle to facilitate his criminal activities.

Text Messages between CI and MERRITT

31. After the CI's arrest, case agents reviewed the contents of the CI's cell phone pursuant to the CI's consent. Located in the CI's cell phone was a contact under the name of "Ric MW 100," which contact the CI identified as MERRITT. The phone number under the contact was 414-317-0845. Text message communications between MERRITT and the CI dated back to at least August of 2022.

32. Generally, the CI and MERRITT did not directly discuss controlled substance trafficking in explicit terms, but their communications reflect their plans to meet on various occasions. For example, on August 17, 2022, the CI texted MERRITT, "I will be up there tonight bro." On October 2, 2022, the CI texted MERRITT, "Can you send me 320?" MERRITT responded, "Yeah I gotchu in the morning tho big dawg." The CI stated, "I'm coming that way tomorrow." MERRITT replied, "Oh that's cool." On

November 30, 2022, the CI texted MERRITT, "Call me I'm up here bro." On December 16, 2022, MERRITT texted the CI a photograph of his (MERRITT's) Wisconsin driver's license.

33. On August 20, 2022, MERRITT texted the CI, "You want something to eat from downstairs??" As previously stated, MERRITT operates a café below his apartment. Case agents believe that this text message further establishes that MERRITT lives above the café at the **SUBJECT PREMISES**.

34. The CI stated that after December of 2022, MERRITT began to use Facetime to communicate with the CI and they would rarely communicate via text message.

SUBJECT PREMISES and Vehicle Information

35. Case agents contacted a representative of WE Energies and found that utilities are registered to MERRITT for Fast Break Café (551 West Becher Street) and for **Apartment A** and **Apartment B**.

36. Case agents conducted a check of a law enforcement database for individuals that were associated with the **SUBJECT PREMISES**. Case agents found that Ricky T. MERRITT (06/15/1985) is associated with the **SUBJECT PREMISES** as well as the café located below the **SUBJECT PREMISES**. A Wisconsin Department of Motor Vehicle check of MERRITT found that his registered address is **551 West Becher Street**. Case agents were able to observe a Wisconsin Department of Motor Vehicle photograph of MERRITT. Case agents further found that MERRITT is on active supervision with the Wisconsin Department of Corrections (WI DOC) and his registered address with WI DOC is **551 West Becher Street #B**. MERRITT is on supervision for a felony conviction of

possession of controlled substances (possession of narcotic drugs and possession of cocaine), *State of Wisconsin vs. Ricky Tyrone Merritt*, Milw. County Case Number 2019CF002159.

37. Case agents located scene photographs from an incident that occurred inside of the **SUBJECT PREMISES** in 2013. Upon reviewing these photographs, case agents found that the southernmost apartment door had the letter “B” on it while the northernmost apartment door had the letter “A” on it. However, the CI stated that currently the doors to the apartments do not have the letters “A” or “B” on them. Although the 2013 incident is a decade ago, case agents believe that the apartments would not have changed letters, even if the doors no longer display any labels.

38. Based on case agents’ training, experience, and familiarity with this investigation, they know that drug traffickers may use dogs to protect themselves and their contraband, and that they may also stash controlled substances, U.S. currency, and/or firearms in separate locations so as to reduce the risk of loss due to theft or law enforcement seizure. According to the CI, MERRITT walks between both **Apartments A** and **B** and carries his firearm into both **Apartments**. As evidenced by WE Energies records, surveillance, and CI information, case agents believe that MERRITT has access to and control over **Apartments A** and **B**, and that MERRITT uses **Apartments A** and **B** as his residence.

39. Through digital surveillance, on March 7, 2023, case agents observed a white **Dodge Durango** bearing **Indiana registration plates of FL386ACC** (VIN# 1C4SDJCT4PC553719) parked on South 5th Place on the East side of the street and directly

across from the ground access door of the **SUBJECT PREMISES**. The white **Dodge Durango** has been determined to be a rental vehicle that is owned by PV Holding (Avis Rental Car). On March 8, 2023, case agents know MERRITT had a meeting with his Wisconsin Department of Corrections agent at 3073 South Chase Avenue. Case agents conducted physical surveillance of MERRITT. At 10:26 a.m., MERRITT left his meeting and walked north from the location towards a Little Caesars pizza restaurant located on east side of South Chase Avenue, where the white **Dodge Durango** was parked. Case agents observed MERRITT enter the white **Dodge Durango** with Indiana plates through the front passenger door. Shortly thereafter, case agents observed the Dodge Durango arrive back at the **SUBJECT PREMISES** through digital surveillance. Case agents observed MERRITT exited the **Durango** with a large bag of what appeared to be dog food. MERRITT then entered the ground entry door to the **SUBJECT PREMISES**.

40. On March 9, 2023, through digital surveillance, case agents observed MERRITT arrive at the **SUBJECT PREMISES** in the white **Dodge Durango** and enter the ground entry door to the **SUBJECT PREMISES**. At approximately 12:08 p.m., case agents observed MERRITT and an unidentified male exit the **SUBJECT PREMISES** and enter the white **Dodge Durango**. MERRITT was the driver of the vehicle and the unidentified male was the front passenger. MERRITT was observed using the vehicle throughout the day on March 9, 2023.

Controlled Delivery of Heroin/Fentanyl

41. On March 6, 2023, under the direction of law enforcement, the CI went to the **SUBJECT PREMISES** to meet with MERRITT. The CI stated that the meeting

occurred in MERRITT's northernmost apartment, **Apartment A**. The CI recorded this conversation in which the CI asked what day MERRITT could meet with the CI. MERRITT told the CI "it's around" and they can meet whenever. The CI told MERRITT that the CI would meet with MERRITT on March 9, 2023.

42. Based on case agents training, experience, and knowledge of the investigation, case agents believe that MERRITT told the CI that he, MERRITT, can get the controlled substances whenever the CI needs it as MERRITT stated, "it's around."

43. In a subsequent conversation between the CI and MERRITT over FaceTime, which was not recorded because MERRITT called the CI when law enforcement was not present, the CI ordered 300 grams of heroin/fentanyl at the direction of case agents.

44. On March 8, 2023, MERRITT informed the CI that he (MERRITT) did not yet have the narcotics to distribute to the CI on March 9, 2023. The CI and MERRITT re-scheduled their meeting for March 13, 2023.

45. On March 13, 2023, at approximately 10:15 a.m., the CI called MERRITT at phone number 414-317-0845 to inform MERRITT he was on his way. Thereafter, case agents met with the CI to purchase heroin/fentanyl from MERRITT at a pre-determined meeting location. Case agents searched the CI for contraband, U.S. currency, and drugs, and located none. Case agents also provided the CI with a recording device. The CI drove to and parked in the area of 7th and Beecher Street. The CI exited the vehicle and entered the southeast door to the **SUBJECT PREMISES**.

46. Preceding the CI's entry in the **SUBJECT PREMISES**, at approximately 9:55 a.m., digital surveillance depicted MERRIT exit the white **Dodge Durango** and enter the **SUBJECT PREMISES**, where he remained through the CI's arrival and entry into the **SUBJECT PREMISES**.

47. According to the CI, the CI stated that he entered **Apartment A** and MERRITT began to break off the heroin/fentanyl from a kilogram-sized amount of fentanyl. The CI stated they went to separate room in **Apartment A** where the CI observed a 20-ton kilogram press, which MERRITT was using to press the heroin/fentanyl that he broke off for the CI. During their meeting, the CI and MERRITT went into **Apartment B**, and the CI noted it was sparsely furnished. The CI observed 4 dogs inside Apartment B. The CI reported that during their meeting, MERRITT was armed with a black and gray handgun on his waistband, and MERRITT later put it into a satchel that he was wearing across his chest. Ultimately, the CI obtained two plastic bags of suspected heroin/fentanyl from MERRITT in **Apartment A**.

48. While the CI was inside the **SUBJECT PREMISES**, case agents were simultaneously listening to the audio recording device previously given to the CI, and they could hear noises consistent with a press being used to press controlled substances. According to what case agents detected through the recording, the recording was consistent with the CI's report of what occurred while inside the **SUBJECT PREMISES**.

49. Following the controlled buy operation, case agents met with the CI at a pre-determined meet location, where the CI turned over to agents two plastic baggies containing suspected heroin/fentanyl. Case agents searched the CI after the controlled

buy operation and did not locate U.S. currency, drugs, or weapons. According to field testing, the substance in one bag contained fentanyl and weighed 224.41 grams. According to field testing, the substance in the second bag contained fentanyl and weighed 63.97 grams. The total weight of the substance the CI obtained from MERRITT in **Apartment A**, which substance tested positive for fentanyl, was approximately 287.38 grams.

50. Based on the foregoing, case agents believe that MERRITT possesses controlled substances in the **SUBJECT PREMISES**.

TECHNICAL TERMS

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

49. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the

data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

51. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and

when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is

analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may

indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site.

Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

53. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence

described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC UNLOCK

54. The warrant I am applying for would permit law enforcement to obtain from MERRITT the display of physical biometric characteristics (such as fingerprint, thumbprint, facial, or iris characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

55. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

56. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button

(often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

57. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

58. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device through his or her irises. For example, Samsung offers an Iris Scanner, which uses the biometric information of an individuals’ irises to identify the user.

59. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

60. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

61. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered within a certain period of time. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

62. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of

MERRITT to the fingerprint scanner of the device; (2) hold the device in front of MERRITT's face to activate the facial recognition feature; and/or (3) hold the device in front of MERRITT's face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

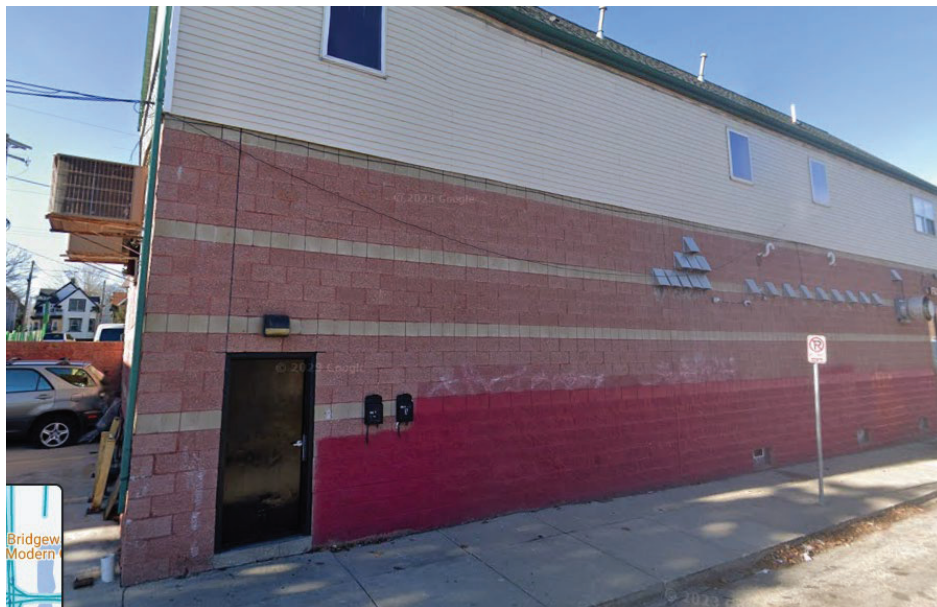
CONCLUSION

63. Based upon the facts contained within this affidavit I believe there is probable cause for a warrant to search the **SUBJECT PREMISES** described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to Be Searched

551 West Becher Street, #A and #B, Milwaukee, Wisconsin, to include all associated common spaces, basement, garage, outbuildings, and a **Dodge Durango bearing Indiana registration plates of FL386ACC**, at this address. Apartments #A and #B are located on the second floor of a dwelling and above two businesses. The ground entry door is on the east side of the building near the south corner. There is a staircase upon opening the ground entry door that runs north to south. Once at the top of the stairs, there is a door to the left and a door straight ahead. The door straight ahead is Apartment #A, while the door to the left is Apartment #B. Apartment #A occupies the northern part of the second floor while Apartment #B occupies the southern part of the second floor.



(Ground access door)



(North side of Building)



(2013 Photograph – Apartment #A straight ahead and Apartment# B on left)

ATTACHMENT B

Property to be seized

1. Evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Section 841(a)(1) (Distribution of and possession with intent to distribute controlled substances), and 846 (Conspiracy to distribute and possess with intent to distribute controlled substances), those violations involving Ricky T. MERRITT, including:

- a. Controlled substances, controlled substance analogues, or listed chemicals;
- b. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
- c. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;
- d. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
- e. Firearms, ammunition, magazines, gun boxes, firearm purchase records or receipts, and other paraphernalia associated with firearms;
- f. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;
- g. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and

other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

- h. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
 - i. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
 - j. Cellular telephones, Smartphones, text messaging systems, and other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;
 - k. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;
 - l. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;
 - m. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances; and
2. Computers, cellular telephones, or storage media used as a means to commit the violations described above;
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in

which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MERRITT to the fingerprint scanner of a device found at the premises; and/or (2) hold a device found at the premises in front of MERRITT’s face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.